Elementy teorii liczb

dr inż. Bartłomiej Pawlik

23 kwietnia 2024

Słowniczek

$\lvert x \rvert$	wartość bezwzględna liczby x
$\mathrm{NWD}(a, b)$	największy wspólny dzielnik liczb a i b
$\mathrm{NWW}(a, b)$	najmniejsza wspólna wielokrotność liczb a i b
$\min\{a, b\}$	niewiększa z liczb a i b
$\max\{a, b\}$	niemniejsza z liczb a i b
$a \mid b$	liczba a jest dzielnikiem liczby b
$a \perp b$	liczby a i b są względnie pierwsze
$\mathbb{N}$	zbiór liczb naturalnych, $\mathbb{N} = \{1, 2, 3, \ldots\}$
$\mathbb{Z}$	zbiór liczb całkowitych, $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$
$\mathbb{Z}_n$	zbiór reszt z dzielenia przez n, $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$
$\mathbb{P}$	zbiór liczb pierwszych
p_i	i-ta liczba pierwsza

Definicja NWD

Niech $a, b \in \mathbb{Z}$ i niech co najmniej jedna z nich jest różna od 0. Liczbę naturalną d nazywamy **największym wspólnym dzielnikiem** liczb a i b, gdy

- $d|a$ i $d|b$,
- jeżeli dla $c \in \mathbb{N}$ mamy $c|a$ i $c|b$, to $c|d$.

Największy wspólny dzielnik liczb a i b oznaczamy jako $\mathrm{NWD}(a, b)$.

Przykład

$\mathrm{NWD}(6, 8) = 2$, $\mathrm{NWD}(14, -17) = 1$, $\mathrm{NWD}(-3, -9) = 3$, $\mathrm{NWD}(0, 24) = 24$.

Definicja NWW

Niech $a, b \in \mathbb{Z}/\{0\}$. Liczbę $D \in \mathbb{N}$ nazywamy **najmniejszą wspólną wielokrotnością** liczb a i b, gdy

- $a|D$ i $b|D$,
- jeżeli dla $c \in \mathbb{N}$ mamy $a|c$ i $b|c$, to $D|c$.

Najmniejszą wspólną wielokrotność liczb a i b oznaczamy jako $\mathrm{NWW}(a, b)$.

Przykład

$\mathrm{NWW}(6, 8) = 24$, $\mathrm{NWW}(14, -17) = 238$, $\mathrm{NWW}(-3, -9) = 9$.

W literaturze często można spotkać się z oznaczeniami $\mathrm{NWD}(a, b) = (a, b)$ i $\mathrm{NWW}(a, b) = [a, b]$.

Własności NWD i NWW

Niech $a, b \in \mathbb{Z}/\{0\}$ i $q \in \mathbb{Z}$.

1. Jeżeli $a|b$, to NWD$(a, b) = |a|$ i NWW$(a, b) = |b|$.
2. NWD$(a, b) =$ NWD$(|a|, |b|)$ i NWW$(a, b) =$ NWW$(|a|, |b|)$.
3. NWD$(a, b) =$ NWD$(a - qb, b)$.
4. NWD$(a, b) \cdot$ NWW$(a, b) = |a \cdot b|$.

Wyznaczenie NWW i NWD

Twierdzenie

Niech

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k} \quad \text{oraz} \quad b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k}.$$

Wtedy

$$NWD(a,b) = p_1^{\min\{\alpha_1,\beta_1\}} \cdot p_2^{\min\{\alpha_2,\beta_2\}} \cdot \ldots \cdot p_k^{\min\{\alpha_k,\beta_k\}}$$

oraz

$$NWW(a,b) = p_1^{\max\{\alpha_1,\beta_1\}} \cdot p_2^{\max\{\alpha_2,\beta_2\}} \cdot \ldots \cdot p_k^{\max\{\alpha_k,\beta_k\}}.$$

Przykład

Wyznaczyć największy wspólny dzielnik oraz najmniejszą wspólną wielokrotność liczb 48 i 180.
Zauważmy, że $48 = 2^4 \cdot 3$ oraz $180 = 2^2 \cdot 3^2 \cdot 5$.
Zatem

$$\mathrm{NWD}(48, 180) = 2^{\min\{4,2\}} \cdot 3^{\min\{1,2\}} \cdot 5^{\min\{0,1\}} = 2^2 \cdot 3^1 \cdot 5^0 = 12$$

oraz

$$\mathrm{NWW}(48, 180) = 2^{\max\{4,2\}} \cdot 3^{\max\{1,2\}} \cdot 5^{\max\{0,1\}} = 2^4 \cdot 3^2 \cdot 5^1 = 720.$$

Przedstawiona metoda nie jest efektywna (ponieważ wymaga rozkładu na czynniki). NWD można obliczyć szybciej korzystając z algorytmu Euklidesa.

Algorytm Euklidesa dla NWD

Niech $a, b \in \mathbb{N}$ i $a > b$.
Po podzieleniu z resztą a przez b otrzymujemy $a = q_1 b + r_1$.
Jeżeli $r_1 = 0$, to $\mathrm{NWD}(a, b) = b$.
Jeżeli $r_1 \neq 0$, to dzielimy z resztą b przez r_1 i otrzymujemy $b = q_2 r_1 + r_2$.
Procedura kończy się, gdy dla pewnego indeksu n mamy $r_n \neq 0$ oraz $r_{n+1} = 0$.
Wtedy $NWD(a, b) = r_n$.

$$\begin{aligned}
a &= q_1 \cdot b + r_1 & \qquad 0 &< r_1 < b \\
b &= q_2 \cdot r_1 + r_2 & 0 &< r_2 < r_1 \\
r_1 &= q_3 \cdot r_2 + r_3 & 0 &< r_3 < r_2 \\
&\vdots & &\vdots \\
r_{n-2} &= q_n \cdot r_{n-1} + r_n & 0 &< r_n < r_{n-1} \\
r_{n-1} &= q_{n+1} \cdot r_n + 0
\end{aligned}$$

$$\mathrm{NWD}(a, b) = r_n$$

Przykład

Wyznaczyć największy wspólny dzielnik oraz najmniejszą wspólną wielokrotność liczb 48 i 180.
Stosując algorytm Euklidesa otrzymujemy

$$
\begin{aligned}
180 &= 3 \cdot 48 + 36 \\
48 &= 1 \cdot 36 + 12 \\
36 &= 3 \cdot 12
\end{aligned}
$$

Zatem $\mathsf{NWD}(48, 180) = 12$.

Z faktu $\mathsf{NWD}(a, b) \cdot \mathsf{NWW}(a, b) = |a \cdot b|$ otrzymujemy $\mathsf{NWW}(a, b) = \dfrac{|a \cdot b|}{\mathsf{NWD}(a, b)}$.
Zatem

$$NWW(48, 180) = \frac{48 \cdot 180}{12} = \frac{4 \cdot 180}{1} = 720.$$

Poprawność algorytmu Euklidesa

- Algorytm produkuje malejący ciąg liczb całkowitych nieujemnych $r_1 > r_2 > \ldots > r_n$ (jedna liczba w jednym kroku). Zatem algorytm zatrzymuje się po skończonej liczbie kroków (nie większej niż wartość r_1).
- Z własności $\mathsf{NWD}(a,b) = \mathsf{NWD}(a-qb,b)$ otrzymujemy

$$\begin{aligned}\mathsf{NWD}(a,b) = \mathsf{NWD}(b,r_1) = \mathsf{NWD}(r_1,r_2) = \ldots = \mathsf{NWD}(r_{n-1},r_n) = \\ = \mathsf{NWD}(r_n,0) = r_n\end{aligned}$$

Twierdzenie (NWD jako kombinacja liniowa)

Dla $a, b \in \mathbb{Z}$ takich, że co najmniej jedna z nich jest różna od 0, istnieją $u, v \in \mathbb{Z}$ takie, że

$$\mathrm{NWD}(a, b) = u \cdot a + v \cdot b.$$

Ponadto $\mathrm{NWD}(a, b)$ jest najmniejszą możliwą <u>dodatnią</u> kombinacją liniową a i b.

Przykład

Wyznaczyć najmniejszą dodatnią kombinację liniową liczb 3 i 7 oraz podać jej przykładowe współczynniki.

$$\begin{aligned}\mathrm{NWD}(3,7) = {} & 1 = 5 \cdot 3 - 2 \cdot 7 \\ & 1 = (-2) \cdot 3 + 1 \cdot 7 \\ & 1 = (-23) \cdot 3 + 10 \cdot 7\end{aligned}$$

Odwrotny algorytm Euklidesa

Algorytm służy wyznaczenia u i v takich, że $a \cdot u + b \cdot v = \mathrm{NWD}(a, b)$.

- Obliczamy $\mathrm{NWD}(a, b)$ korzystając z algorytmu Euklidesa otrzymując ciąg równań
  $a = q_1 \cdot b + r_1, \quad b = q_2 \cdot r_1 + r_2, \quad r_1 = q_3 \cdot r_2 + r_3, \quad \dots,$
  $r_{n-3} = q_{n-1} \cdot r_{n-2} + r_{n-1}, \quad r_{n-2} = q_n \cdot r_{n-1} + r_n, \quad r_{n-1} = q_{n+1} \cdot r_n.$
- Z i-tego równania wyznaczamy wartość r_i dla każdego $i = 1, 2, \dots, n$ (więc pomijamy ostatnie równanie).
- Wyliczone r_n daje nam równanie
  $\mathrm{NWD}(a, b) = r_{n-2} - q_n \cdot r_{n-1}.$
  Do tego równania wstawiamy wyliczoną wartość r_{n-1} (w ten sposób otrzymujemy $\mathrm{NWD}(a, b)$ w kombinacji liniowej r_{n-2} i r_{n-3}).
- Kontynuujemy podstawianie r_{n-2}, r_{n-3} itd. aż do r_1, po drodze upraszczając współczynniki. W efekcie dostajemy zapis implikujący wartości u i v.

Definicja

Liczba $n \in \mathbb{N}$ jest **liczbą pierwszą**, jeżeli n ma dokładnie dwa dodatnie dzielniki.

- 0 nie jest liczbą pierwszą (po pierwsze nie jest liczbą dodatnią, a po drugie ma nieskończenie wiele dzielników).
- 1 nie jest liczbą pierwszą (ma dokładnie jeden dodatni dzielnik).
- Początkowe liczby pierwsze: $2, 3, 5, 7, 11, 13, 17, 19, 23$.
- Liczby naturalne <u>większe od 1</u> dzielimy na liczby pierwsze i liczby złożone (złożone to te, które nie są pierwsze).
- 1 nie jest ani liczbą pierwszą, ani liczbą złożoną.
- Zbiór liczb pierwszych oznaczamy przez $\mathbb{P}$.

Twierdzenie

Liczb pierwszych jest nieskończenie wiele.

Dowód.

Załóżmy nie wprost, że teza twierdzenia jest fałszywa, tj. zbiór liczb pierwszych jest skończony. Zatem dla pewnej liczby naturalnej n mamy

$$\mathbb{P} = \{p_1, p_2, \ldots, p_n\}.$$

Niech P będzie następnikiem iloczynu wszystkich elementów powyższego zbioru $\mathbb{P}$:

$$P = 1 + \prod_{i=1}^{n} p_i.$$

Zauważmy, że liczba P przy dzieleniu przez p_i (dla $i = 1, 2, \ldots, n$) daje resztę 1, zatem liczba P nie jest podzielna przez żadną liczbę pierwszą — uzyskaliśmy sprzeczność. $\square$

Powyższy dowód ma ∼2500 lat (*Elementy* Euklidesa).

Czy z powyższego dowodu wynika, że liczba P jest liczbą pierwszą? Nie!

$$
\begin{aligned}
2 + 1 &= 3 \in \mathbb{P} \\
2 \cdot 3 + 1 &= 7 \in \mathbb{P} \\
2 \cdot 3 \cdot 5 + 1 &= 31 \in \mathbb{P} \\
2 \cdot 3 \cdot 5 \cdot 7 + 1 &= 211 \in \mathbb{P} \\
2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 &= 2311 \in \mathbb{P} \\
2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 &= 59 \cdot 509 \\
2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 + 1 &= 19 \cdot 97 \cdot 277 \\
2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 + 1 &= 347 \cdot 27\,953 \\
2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 + 1 &= 317 \cdot 703\,763 \\
2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 + 1 &= 331 \cdot 571 \cdot 34\,231 \\
2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 + 1 &= 200\,560\,490\,131 \in \mathbb{P} \\
2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 + 1 &= 181 \cdot 60\,611 \cdot 676\,421
\end{aligned}
$$

Zatem konstrukcja w powyższym dowodzie nie daje przepisu na tworzenie coraz większych liczb pierwszych, a jedynie wskazuje, że istnieją liczby pierwsze nienależące do dowolnego skończonego zbioru liczb pierwszych.

Liczby o jeden większe od iloczynu początkowych liczb pierwszych to tzw. *liczby Euklidesa*:

$$3,\ 7,\ 31,\ 211,\ 2311,\ 30\,031,\ 510\,511, \ldots$$

Definicja

Liczbę

$$E_n = 1 + \prod_{i=1}^{n} p_i$$

nazywamy n-*tą liczbą Euklidesa*.

Do dzisiaj nie wiadomo czy

- jest nieskończenie wiele liczb pierwszych Euklidesa?
- każda liczba Euklidesa jest bezkwadratowa?

Podstawowe twierdzenie arytmetyki

Każdą liczbę całkowitą dodatnią można przedstawić jako iloczyn liczb pierwszych. Przedstawienie takie jest jednoznaczne z dokładnością do kolejności czynników.

Przykład

$12 = 2 \cdot 2 \cdot 3 = 2 \cdot 3 \cdot 2 = 3 \cdot 2 \cdot 2$

Wniosek

Każda większa od 1 liczba naturalna n może być jednoznacznie zapisana w tzw. **postaci kanonicznej**

$$n = q_1^{\alpha_1} \cdot q_2^{\alpha_2} \cdot \ldots \cdot q_k^{\alpha_k},$$

gdzie q_i są liczbami pierwszymi, α_i są liczbami naturalnymi oraz $q_1 < q_2 < \ldots < q_k$.

Przykład

Postacią kanoniczną liczby 12 jest $2^2 \cdot 3$.

Funkcja φ-Eulera

Definicja

Liczby całkowite a i b nazywamy **względnie pierwszymi**, gdy $\mathrm{NWD}(a, b) = 1$.

Zapis $a \perp b$ oznacza, że a i b są liczbami względnie pierwszymi.

Stwierdzenie

Liczby $\dfrac{a}{\mathrm{NWD}(a,b)}$ i $\dfrac{b}{\mathrm{NWD}(a,b)}$ są względnie pierwsze.

Przykład

$\mathrm{NWD}(48, 180) = 12$, więc 48 i 180 nie są liczbami względnie pierwszymi.

$$\frac{48}{12} = 4, \quad \frac{180}{12} = 15.$$

Zauważmy, że $\mathrm{NWD}(4, 15) = 1$. Zatem $4 \perp 15$.

Definicja

Dla każdej liczby $n \in \mathbb{N}/\{1\}$ określamy liczbę $\varphi(n)$ jako liczbę dodatnich liczb całkowitych mniejszych od n i względnie pierwszych z n:

$$\varphi(n) = \Big|\{1 \leqslant k < n : \, k \perp n\}\Big|.$$

Funkcję $\varphi = \varphi(n)$ nazywamy **funkcją φ-Eulera**.

Przykład

Obliczmy NWD$(k, 12)$ dla k mniejszych od 12:

$$\begin{array}{llll} \text{NWD}(1,12) = 1, & \text{NWD}(4,12) = 4, & \text{NWD}(7,12) = 1, & \text{NWD}(10,12) = 2, \\ \text{NWD}(2,12) = 2, & \text{NWD}(5,12) = 1, & \text{NWD}(8,12) = 4, & \text{NWD}(11,12) = 1. \\ \text{NWD}(3,12) = 3, & \text{NWD}(6,12) = 6, & \text{NWD}(9,12) = 3, & \end{array}$$

Zatem

$$\varphi(12) = \Big|\{1, 5, 7, 11\}\Big| = 4.$$

Stwierdzenie

Dla dowolnej liczby pierwszej p i liczby całkowitej dodatniej α zachodzi:

- $\varphi(p) = p - 1$,
- $\varphi(p^\alpha) = p^\alpha \cdot \left(1 - \frac{1}{p}\right)$.

Dowód.

- Liczba pierwsza p jest względnie pierwsza z każdą z liczb $1, 2, \ldots, p - 1$.
- Zauważmy, że jedynie wielokrotności liczby pierwszej p mają wspólny nietrywialny dzielnik z p^α. Zatem w zbiorze $\{1, 2, \ldots, p^\alpha - 1\}$ liczbami niebędącymi liczbami względnie pierwszymi z p^α są

$$1 \cdot p,\ 2 \cdot p,\ \ldots,\ (p^{\alpha-1} - 1) \cdot p,$$

więc ich liczba wynosi $p^{\alpha-1} - 1$. Zatem

$$\varphi\left(p^\alpha\right) = \left(p^\alpha - 1\right) - \left(p^{\alpha-1} - 1\right) = p^\alpha - p^{\alpha-1} = p^\alpha \left(1 - \frac{1}{p}\right).$$

□

Stwierdzenie

Jeżeli $a \perp b$, to $\varphi(ab) = \varphi(a)\varphi(b)$.

Z dwóch ostatnich stwierdzeń wynika następujące

Twierdzenie

Niech $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ będzie postacią kanoniczną liczby $n \in \mathbb{N}/\{1\}$. Wtedy

$$\varphi(n) = n \cdot \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

Przykład

Wyznaczyć liczby $\varphi(180)$ i $\varphi(12\,936)$.

- Postać kanoniczna liczby 180 to $2^2 \cdot 3^2 \cdot 5$, więc jedynymi dzielnikami pierwszymi danej liczby są 2, 3 i 5. Zatem

$$\varphi(180) = 180 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 48.$$

- $12\,936 = 2^3 \cdot 3 \cdot 7^2 \cdot 11$, więc dzielnikami pierwszymi danej liczby są 2, 3, 7 i 11. Zatem

$$\varphi(12\,936) = 12\,936 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{6}{7} \cdot \frac{10}{11} = 3360.$$

Współczynniki rozkładu silni

Twierdzenie

Niech n będzie liczbą całkowitą dodatnią i niech $\alpha_p(N)$ oznacza największą potęgę liczby p dzielącą liczbę N. Wtedy

$$\alpha_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \ldots = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor .$$

Przykład

Wskaż największą potęgę liczby 3 dzieląca liczbę $100!$

Korzystając z powyższego wzoru mamy

$$\alpha_3(100!) = \left\lfloor \frac{100}{3} \right\rfloor + \left\lfloor \frac{100}{9} \right\rfloor + \left\lfloor \frac{100}{27} \right\rfloor + \left\lfloor \frac{100}{81} \right\rfloor + \left\lfloor \frac{100}{243} \right\rfloor + \ldots =$$
$$= 33 + 11 + 3 + 1 + 0 + \ldots = 48.$$

Zatem szukana potęga to 3^{48}.

Twierdzenie

Dla każdej liczby pierwszej p i dla każdej liczby całkowitej dodatniej n zachodzi

$$\alpha_p(n!) < \frac{n}{p-1}$$

Dowód.

$$\alpha_p(n!) < \frac{n}{p} + \frac{n}{p^2} + \frac{n}{p^3} + \ldots = \frac{n}{p}\left(1 + \frac{1}{p} + \frac{1}{p^2} + \ldots\right) = \frac{n}{p} \cdot \frac{p}{p-1} = \frac{n}{p-1}$$

$\square$